

AMENDMENT

In the Claims:

Please cancel claims 1-24 without prejudice and add the following claims.

SUB B7

25. A method for managing encryption within a database system,
2 wherein encryption is performed automatically and transparently to a user of the
3 database system, the method comprising:
4 receiving a request at the database system to store data in the database
5 system;
6 wherein the request is directed to storing data in a portion of the database
7 system that has been designated as encrypted;
8 in response to receiving the request, automatically encrypting data within
9 the database system using an encryption function to produce an encrypted data;
10 and
11 storing the encrypted data in the database system.

26. The method of claim 25,
2 wherein the portion of the database system that has been designated as
3 encrypted includes a column of the database system;
4 wherein the encryption function uses a key stored in a keyfile managed by
5 a security administrator; and
6 wherein the encrypted data is stored using a storage function of the
7 database system.

27. The method of claim 26, further comprising:

2 receiving a request to retrieve data from the column of the database
3 system;
4 if the request to retrieve data is received from a database administrator,
5 preventing the database administrator from decrypting the encrypted data;
6 if the request to retrieve data is received from the security administrator,
7 preventing the security administrator from decrypting the encrypted data; and
8 if the request to retrieve data is from an authorized user of the database
9 system, allowing the authorized user to decrypt the encrypted data.

1 28. The method of claim 26, wherein the security administrator selects
2 one of, data encryption standard (DES) and triple DES as a mode of encryption
3 for the column.

a'
1 29. The method of claim 26, wherein the security administrator, a
2 database administrator, and a user administrator are distinct roles, and wherein a
3 person selected for one of these roles is not allowed to be selected for another of
4 these roles.

1 30. The method of claim 26, wherein managing the keyfile includes,
2 but is not limited to:
3 creating the keyfile;
4 establishing a plurality of keys to be stored in the keyfile;
5 establishing a relationship between a key identifier and the key stored in
6 the keyfile;
7 storing the keyfile in one of,
8 an encrypted file in the database system, and
9 a location separate from the database system; and

10 moving an obfuscated copy of the keyfile to a volatile memory within a
11 server associated with the database system.

1 31. The method of claim 30, wherein the key identifier associated with
2 the column is stored as metadata associated with a table containing the column
3 within the database system.

1 32. The method of claim 30, further comprising establishing
2 encryption parameters for the column, wherein encryption parameters include
3 encryption mode, key length, and integrity type by:
4 entering encryption parameters for the column manually; and
5 recovering encryption parameters for the column from a profile table in the
6 database system.

a' 1 33. The method of claim 26, wherein upon receiving a request from the
2 security administrator specifying the column to be encrypted, if the column
3 currently contains data, the method further comprises:
4 decrypting the column using an old key if the column was previously
5 encrypted; and
6 encrypting the column using a new key.

1 34. A computer-readable storage medium storing instructions that
2 when executed by a computer causes the computer to perform a method for
3 managing encryption within a database system, wherein encryption is performed
4 automatically and transparently to a user of the database system, the method
5 comprising:
6 receiving a request at the database system to store data in the database
7 system;

8 wherein the request is directed to storing data in a portion of the database
9 system that has been designated as encrypted;
10 in response to receiving the request, automatically encrypting data within
11 the database system using an encryption function to produce an encrypted data;
12 and
13 storing the encrypted data in the database system.

a' 1 35. The computer-readable storage medium of claim 34,
2 wherein the portion of the database system that has been designated as
3 encrypted includes a column of the database system;
4 wherein the encryption function uses a key stored in a keyfile managed by
5 a security administrator; and
6 wherein the encrypted data is stored using a storage function of the
7 database system.

1 36. The computer-readable storage medium of claim 35, the method
2 further comprising:
3 receiving a request to retrieve data from the column of the database
4 system;
5 if the request to retrieve data is received from a database administrator,
6 preventing the database administrator from decrypting the encrypted data;
7 if the request to retrieve data is received from the security administrator,
8 preventing the security administrator from decrypting the encrypted data; and
9 if the request to retrieve data is from an authorized user of the database
10 system, allowing the authorized user to decrypt the encrypted data.

1 37. The computer-readable storage medium of claim 35, wherein the
2 security administrator selects one of, data encryption standard (DES) and triple
3 DES as a mode of encryption for the column.

1 38. The computer-readable storage medium of claim 35, wherein the
2 security administrator, a database administrator, and a user administrator are
3 distinct roles, and wherein a person selected for one of these roles is not allowed
4 to be selected for another of these roles.

a' 1 39. The computer-readable storage medium of claim 35, wherein
2 managing the keyfile includes, but is not limited to:
3 creating the keyfile;
4 establishing a plurality of keys to be stored in the keyfile;
5 establishing a relationship between a key identifier and the key stored in
6 the keyfile;
7 storing the keyfile in one of,
8 an encrypted file in the database system, and
9 a location separate from the database system; and
10 moving an obfuscated copy of the keyfile to a volatile memory within a
11 server associated with the database system.

1 40. The computer-readable storage medium of claim 39, wherein the
2 key identifier associated with the column is stored as metadata associated with a
3 table containing the column within the database system.

1 41. The computer-readable storage medium of claim 39, wherein the
2 method further comprises establishing encryption parameters for the column,

3 wherein encryption parameters include encryption mode, key length, and integrity
4 type by:
5 entering encryption parameters for the column manually; and
6 recovering encryption parameters for the column from a profile table in the
7 database system.

1 42. The computer-readable storage medium of claim 35, wherein upon
2 receiving a request from the security administrator specifying the column to be
3 encrypted, if the column currently contains data, the method further comprises:
4 decrypting the column using an old key if the column was previously
5 encrypted; and
6 encrypting the column using a new key.

21
1 43. An apparatus that facilitates managing encryption within a
2 database system, wherein encryption is performed automatically and transparently
3 to a user of the database system, comprising:
4 a receiving mechanism that is configured to receive a request at the
5 database system to store data in the database system;
6 wherein the request is directed to storing data in a portion of the database
7 system that has been designated as encrypted;
8 an encrypting mechanism that is configured to automatically encrypt data
9 within the database system using an encryption function to produce an encrypted
10 data; and
11 a storing mechanism that is configured to store the encrypted data in the
12 database system.

1 44. The apparatus of claim 43,

2 wherein the portion of the database system that has been designated as
3 encrypted includes a column of the database system;
4 wherein the encryption function uses a key stored in a keyfile managed by
5 a security administrator; and
6 wherein the encrypted data is stored using a storage function of the
7 database system.

21
1 45. The apparatus of claim 44, further comprising:
2 the receiving mechanism that is further configured to receive a request to
3 retrieve data from the column of the database system;
4 an access mechanism that is configured to prevent a database administrator
5 and the security administrator from decrypting the encrypted data; and
6 wherein the access mechanism is configured to allow an authorized user
7 of the database system to decrypt the encrypted data.

1 46. The apparatus of claim 44, further comprising a selection
2 mechanism that is configured to select one of, data encryption standard (DES) and
3 triple DES as a mode of encryption for the column.

1 47. The apparatus of claim 44, wherein the security administrator, a
2 database administrator, and a user administrator are distinct roles, and wherein a
3 person selected for one of these roles is not allowed to be selected for another of
4 these roles.

1 48. The apparatus of claim 44, further comprising:
2 a creating mechanism that is configured to create the keyfile;
3 an establishing mechanism that is configured to establish a plurality of
4 keys to be stored in the keyfile;

5 wherein the establishing mechanism is further configured to establish a
6 relationship between a key identifier and the key stored in the keyfile;
7 wherein the storing mechanism is further configured to store the keyfile in
8 one of,
9 an encrypted file in the database system, and
10 a location separate from the database system; and
11 a moving mechanism that is configured to move an obfuscated copy of the
12 keyfile to a volatile memory within a server associated with the database system.

1 49. The apparatus of claim 48, wherein the key identifier associated
2 with the column is stored as metadata associated with a table containing the
3 column within the database system.

a'
1 50. The apparatus of claim 48, wherein the establishing mechanism is
2 further configured to establish encryption parameters for the column,
3 wherein encryption parameters include encryption mode, key length, and
4 integrity type, and wherein the establishing mechanism includes:
5 an entering mechanism that is configured to enter encryption parameters
6 for the column manually; and
7 a recovering mechanism that is configured to recover encryption
8 parameters for the column from a profile table in the database system.

1 51. The apparatus of claim 44, further comprising:
2 a decrypting mechanism that is configured to decrypt the column using a
3 previous key if the column was previously encrypted; and
4 wherein the encrypting mechanism is further configured to encrypt the
5 column using a new key.